CHELSEA TECHNOLOGIES

“Cybersecurity”

IT is a serious matter

Solomon Soldaner & Kara Deane

September 2016

Introduction: Cyber Security

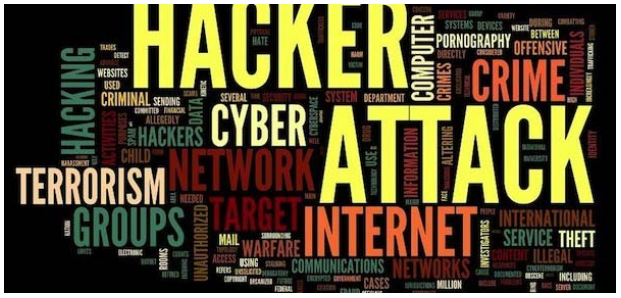
What will we cover?

- What is Cyber Security?
- Understand why it's important for firms of all sizes to address cybersecurity risks.
- Learn about one of the currently most dangerous and disruptive cyber threats affecting businesses today.
- Learn how you can contribute to reducing the risks of data breaches and cyber attacks for your firm.

Cyber Security: Definition

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

Source: James Magdalenski, Director of Naval Operations Security Support Team



Why is Cyber Security Important?

- “90 percent of companies worldwide recognize they are insufficiently prepared to protect themselves against [cyber attacks].” - The World Economic Forum (2015)
- According to the Center for Strategic and International Studies, Cyber crime costs the global economy over US$400 billion per year.
- In 2014, more than 3,000 companies in the United States had their systems compromised by hackers – Washington Post (2014)

Why would they target me?

- **Hackers expect loopholes in small businesses.**
- **You may be opening a back door to a larger company's data.**
- **Recent statistics don't favor you in the slightest.**

Cyber Security: A Serious Matter

- Data breaches are on the rise more than ever (August 2016)
  - 68 Million Dropbox hacked DropBox accounts for sale on the dark Web
  - FTSE 100 Company Sage announces data breach
  - Personal information of Pulse victims (Orlando, FL), survivors breached Ransomware Continues

Types of Cyber Threats

Here's a quick list of just some of the common security threats your impacting businesses today:

- Botnets
- Distributed denial-of-service (DDoS)
- Hacking
- Malware
- Phishing
- Ransomware

Cyber Threat: Ransomware

Ransomware is a type of malicious software (malware) that hijacks all your files, locks them up with unbreakable encryption, and demands a ransom usually in Bitcoins to decrypt them.

Ransomware spreads through e-mail attachments, infected programs and compromised websites. Ransomware malware may also be called a cryptovirus, cryptotrojan or cryptoworm*

*TechTarget 2016

Cyber Threat: Ransomware

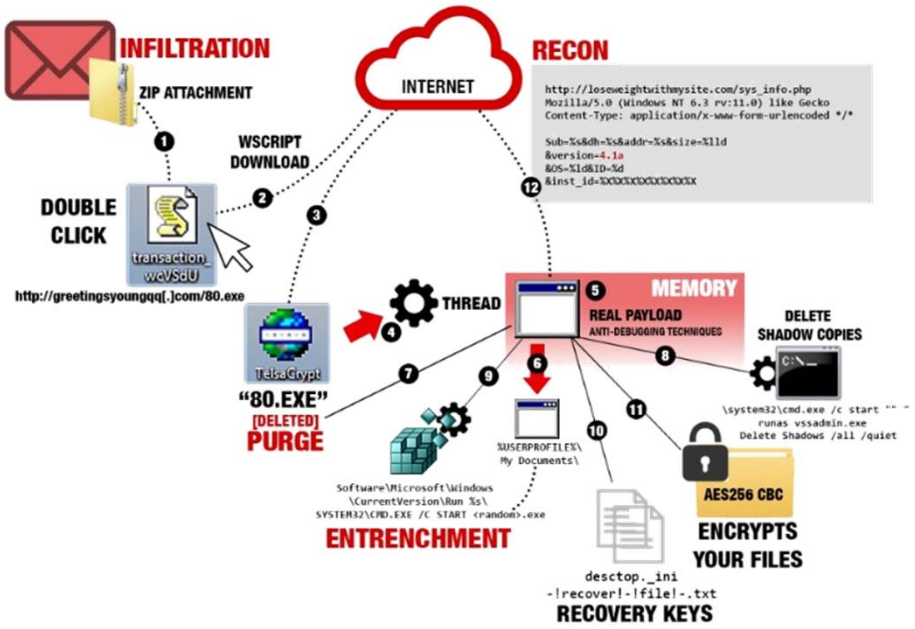
Ransomware is a growing threat impacting businesses of all sizes.

- In the U.S. alone, victims lost $209 million due to ransomware in the first three months of 2016, compared with $24 million in all of 2015, according to the FBI.
- Ransomware is on track to be a $1 billion crime in 2016
- 4,000+ ransomware attacks happened daily since January 1, 2016

Anatomy of Ransomware Attack

5 Main Stages of Ransomware

- Infection
- Contact Headquarters
- Handshake and Keys
- Encryption
- Extortion



Anatomy of Ransomware Attack

Stage 1 – Infection

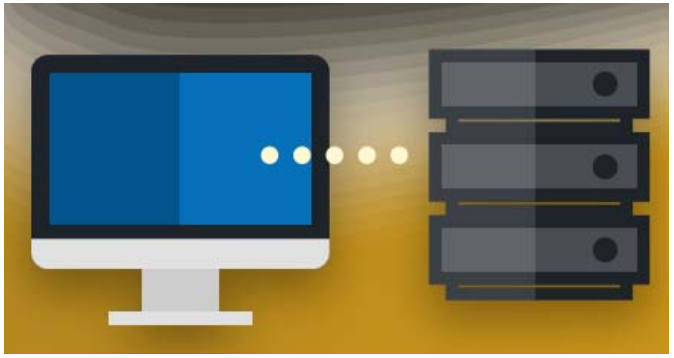
User receives an email that appears to be from their boss or someone they know. It contains an attachment or link to a website that seems legitimate but is actually an infection that is surreptitiously downloading a payload to the user's computer.

Anatomy of Ransomware Attack

Stage 2 – Contacting Headquarters

Before crypto-ransomware starts attacking you, it contacts a server operated by the criminal gang that owns it.

Your infected computer is waiting for further instructions from the criminals to start the encryption



Anatomy of Ransomware Attack

Stage 3 – Handshake and Keys

The ransomware client and server identify each other through a carefully arranged “handshake,” and the server generates two cryptographic keys. One key is kept on your computer, the second key is stored securely on the criminals’ server.

Anatomy of Ransomware Attack

Stage 4 – Encrypt

With the cryptographic keys established, the ransomware on your computer starts encrypting every file it finds with any of dozens of common file extensions, from Microsoft Office documents to .JPG images and more.

Afterwards, it spreads to another computer or server in the network to continue the encryption.

Anatomy of Ransomware Attack

Stage 5 – Extortion

The ransomware displays a screen giving you a time limit to pay up before the criminals destroy the key to decrypt your files. The price, which varies but not high, must be paid in untraceable bitcoins or other electronic payments.

Anatomy of Ransomware Attack

Stage 6 – Now What?

Do you pay?

Do you call a security consultant?

Do you have good backups?

Do you start over?

Staying Safe from Ransomware

- **Lock Down File Permissions**
- **Use Advanced Endpoint Protection**
- **Use Web and Email Protection**
- **Educate Users**:
- **Make Time for testing backups**
- **Disconnect from Network Immediately**

More Safety Steps

- **Backup Backup Backup!**
- **Apply Security Patches and Software Updates**
- **Use Strong Passwords or Two Factor Authentication**
- **Secure your WiFi**
- **Encrypt Laptops and Portable Storage Media**

What should I do right now?

- Ensure you are compliant
- Make Security a priority
- Create a business continuity plan

Q&A

Free Cyber Security Assessment

Set an appointment for a free 1 hour security assessment with our highly skilled security experts.

Kara Deane or Solomon Soldaner
Chelsea Technologies
101 NE Third Ave Suite 1120
Fort Lauderdale, FL 33301
Phone: 954-454-9797
Emails: kdeane@chelsea-tech.com or
ssoldaner@chelsea-tech.com
Web: http://www.chelsea-tech.com